NTT Security

Prevention Is Better Than Cure:

Business Security – The Journey Continues

2018 Risk:Value Report

Executive Summary

Nearly 40 years after the first PC rolled off the production line, the hope is that companies would have a firm grip on information security issues.

This year's Risk:Value Report from NTT Security shows that there is still a lot of work to do. It crystallizes in one shocking statistic: one-third of companies would rather pay a hacker's ransom than invest in information security. Many organizations are still stuck in a reactive mindset when it comes to security.

Working with research agency Vanson Bourne, NTT Security interviewed 1,800 global business decision makers to understand their cybersecurity stance. We found that respondents are still making the same mistakes, failing to make any progress in crucial areas such as cybersecurity awareness and preparedness. Senior management seems distracted when it comes to security, and there is no single executive role that is surfacing as ultimately responsible. It is one more challenge that organizations face in a range of business threats, including economic turbulence, political and regulatory uncertainty, and general day-to-day firefighting.

2018 is a groundbreaking year for information security.

Regulators are now enforcing the General Data Protection Regulation (GDPR). Even now, only one in three respondents globally believe that it affects them. Even in Europe, fewer than half of the respondents in any country thought they were subject to the GDPR.

Any company dealing with data on EU citizens must comply with the GDPR, but countries in other regions must deal with their own regulations too. These include Singapore's Monetary Authority of Singapore Act and Australia's Privacy Amendment (Notifiable Data Breaches) Bill 2016, mandatory data breach reporting legislation which came into force in February 2018.

In the meantime, the threats continue to mount. Breaches at companies including Equifax[1], Verizon[2], and Hudson's Bay Company[3] made the headlines. The numbers of compromised records and the potential effect on victims are growing. Cyber criminals are also concentrating on tried and tested exploits, while continually investigating new ones. Ransomware continues to grow, while further attacks, such as cryptojacking are quickly spreading. In this attack, hackers use compromised servers and endpoints to mine for cryptocurrencies, which are rapidly increasing in value making them a prime target.

The stakes are rising, and companies are often standing still in the race to deal with security threats. This report examines the current state of play among organizations both large and small, across the globe.

The impact of a data breach

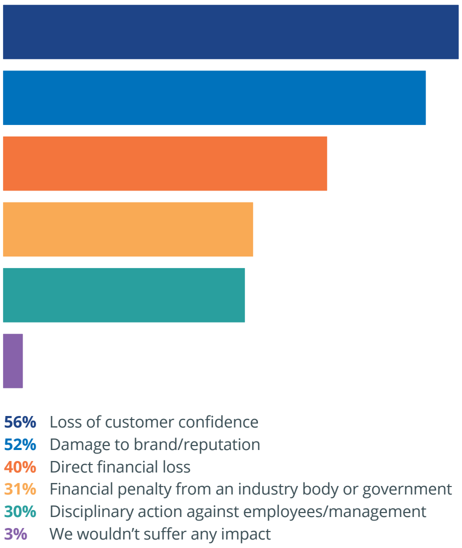
Organizations worry most about how a data breach makes them look

Across the board, companies were most concerned about what a data breach would do to their image, with 56 percent concerned about the loss of customer confidence and 52 percent fretting about damage to brand and reputation. These data breach-related concerns correlate closely with companies' broader fears. One in four (25 percent) saw losing market share to competitors as their biggest threat. Sweden was an outlier here, with 27 percent of companies worrying about a lack of employee skills in key areas.

Some sectors are far more worried about the loss of market share than others. Telecommunications companies, which continuously worry about customer churn, led the pack at 38 percent. Chemicals/petrochemicals/pharmaceuticals came a close second at 36 percent.

The UK stood out for its concern over the effect of data breaches on company image. 73 percent of UK respondents worried about the impact on customer confidence following an information security incident, compared to the 56 percent global average. 69 percent of UK organizations fretted about brand damage, compared to 52 percent globally. Cultural differences are a likely cause.

Figure 1 "If information was stolen in a security breach, how would your organization be affected?"
Asked to all respondents (1,800)



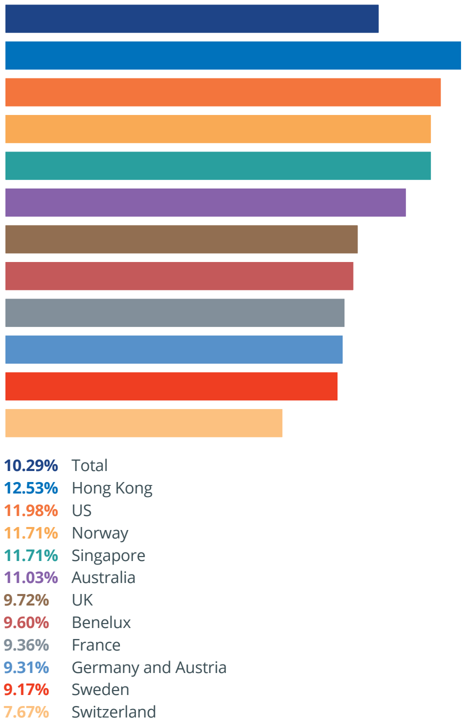
Financial losses came a close second

The economic impacts of a data breach ranked a clear second after image, but even here financial fallout worried some companies more than others. Direct financial losses ranked highest, with 40 percent of companies highlighting it as a concern.

Indirect losses, such as the impact of regulatory penalties and loss of share price, were less of a concern. 31 percent of companies felt that they would be affected by financial penalties, and 29 percent said that they would be affected by loss of shareholder value.

The effect of a breach on revenue has risen only slightly after a downward turn between 2015 and 2017, with the average revenue drop forecast at 10.29 percent. European countries were more optimistic overall, anticipating lower revenue losses than the US and APAC respondents. The exception was Norway, a member of the European Economic Area (EEA), which at 11.71 percent of revenue anticipated higher losses than its EU counterparts.

Figure 2 Analysis showing the average percentage estimated revenue drop due to an information security breach for respondents' organizations. *Asked to all respondents (1,800)*



The cost of recovery continues to rise

While the predicted effect of a data breach on revenues appeared mostly static, the cost of recovery is of greater concern. It has increased to USD 1.52 million today, compared to USD 1.35 million in 2017 and under USD 1 million in 2015. Perhaps most worrying of all, though, is the fact that almost one in four (24 percent) respondents were unable to predict the recovery cost, suggesting a lack of risk analysis in data breach planning.

On average, respondents questioned for the 2018 Risk:Value Report anticipated a 57 day recovery time if targeted by a data breach. Forecasts varied significantly by region, with Singapore most optimistic at 37 days, and Australia most pessimistic at 82 days.

Companies are over-confident about their level of vulnerability

Almost half of all business decision makers (47 percent) said that they had not been affected by data breaches. This assumption is worryingly high, given how difficult it is to prove with certainty that a company has not been breached. Another concern is the one in three respondents who say that they do not expect to suffer from a breach.

The US was the most confident when it comes to data breaches, with 46 percent claiming never to have been breached, and stating that they do not expect to be. The number that didn't know, or didn't think that they had suffered from a breach but anticipated one, was relatively low. In short, US companies were very binary, either sure that they had experienced a breach or confident that they hadn't and never would.

Comparatively, most other countries were willing to admit that they didn't know. This mindset was especially prevalent in the UK, where more than one in five (22 percent) agreed that they didn't know whether they had suffered from a breach or not.

Figure 3 Analysis showing the average estimated cost to respondents' organizations to recover if they suffered a security breach and lost information.
Asked to all respondents (1,800)

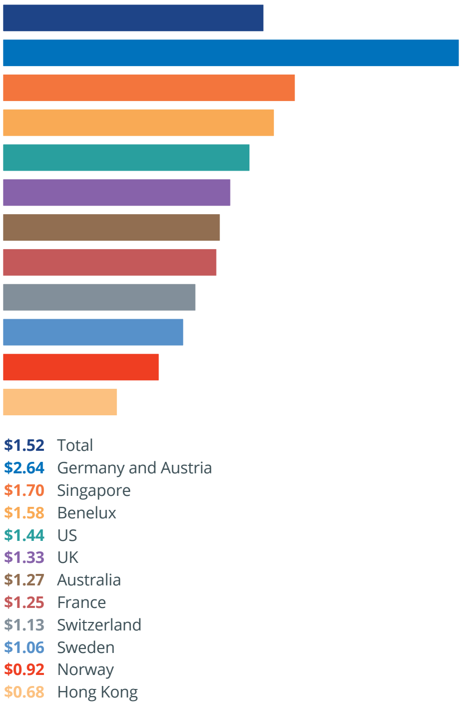
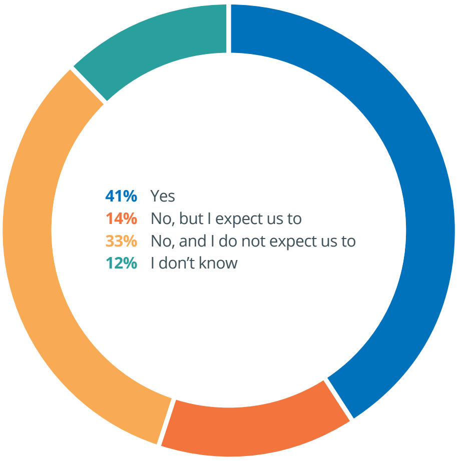


Figure 4 Analysis showing whether or not respondents' organizations have ever suffered an information security breach. *Asked to all respondents (1,800)*



A third of respondents would rather pay a ransom later than invest in protection now

Respondents' refusal to acknowledge the risk of a data breach may help to explain one of the most shocking statistics in this report. NTT Security asked organizations whether they would try to cut costs by paying a hacker's ransom rather than investing in information security. One in three respondents said yes, with a further 16 percent stating that they didn't know! That means only half of all respondents would prefer to invest in IT security rather than taking a reactive approach.

These findings are especially worrying given the rapid growth in ransomware. NTT Security's latest Global Threat Intelligence Report (GTIR) charts a global rise in ransomware detections from one percent in 2016 to seven percent in 2017. It was the leading form of malware in EMEA, constituting 29 percent of all attacks.[4]

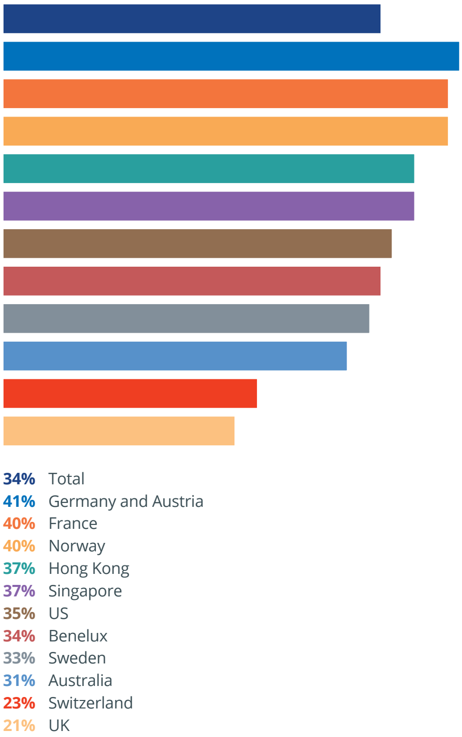
The wait-and-see attitude towards security investment is of particular concern after incidents such as WannaCry and Petya. First, it shows that many companies are still prepared to take a short-term, reactive approach to security to drive down costs, rather than adopting a longer-term, strategic and preventative approach.

Second, there is no guarantee that cyber criminals will honour any ransom that a company pays, and it also serves to feed a damaging criminal enterprise.

Finally, with many ransomware players demanding payment in cryptocurrency, companies that do decide to pay the ransom could render themselves vulnerable to wild swings in asset value.

Digging deeper into this research shows some brighter spots and some considerably darker ones. The UK was a little more sensible than the global average, with fewer respondents prepared to prioritize ransoms over long-term investment. Nevertheless, just over one in five UK respondents (21 percent) were still willing to focus on ransomware payments rather than cybersecurity investments in an attempt to save money.

Figure 5 Analysis showing the percentage of respondents who agree that their organization would consider paying a ransom by a hacker rather than invest in security because it is cheaper, split by respondent country. *Asked to all respondents (1,800)*



No real change in cybersecurity preparedness

IT seems to have plateaued on information security spending. Operations spent more of its budget on information security this year (17.84 percent) than IT did (14.32 percent) for the second year running, widening the gap between the two. Notably, IT spent less of its budget on information security this year than in 2017 (14.58 percent). Operations in the US stood out as particularly big spenders on information security, allocating 21.26 percent of budget to it.

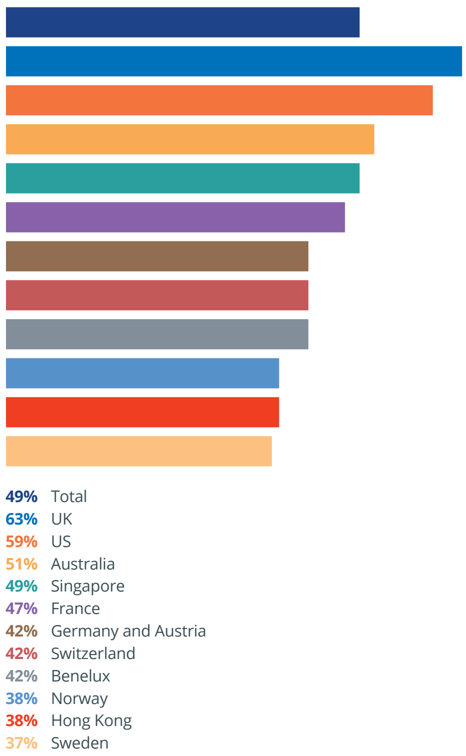
Perhaps this goes some way to explaining the lack of preparedness that we continue to see across the board. More than half (57 percent) of respondents reported having an information security policy in place, barely nudging the dial from 2017's 56 percent. 26 percent say that they are working on it, which again is one percent less than last year.

Respondents haven't done that much better at communicating these policies, either. 81 percent of those with a policy in place said that they had actively relayed it to the rest of the organization, compared to 79 percent last year. It should come as no surprise, then, that the same proportion of respondents as last year think that their employees are fully aware of those policies, just 39 percent.

If companies are not moving the dial when it comes to preparing and communicating security policies, are they perhaps faring better at developing incident response plans to deal with breaches after they happen? 49 percent said that they had implemented such a program, with another 30 percent claiming to be in the process. Last year's count: 48 percent had put one in place, with 31 percent working on it. These figures suggest that one percent of companies have finished a response plan since last year, and still fewer than half have one in place.

The UK, which claims top score for implementing incident response plans (63 percent of respondents) was fourth from bottom in response plan awareness at 44 percent. These plans must be more than shelfware if they are to have an impact.

Figure 6 Analysis showing the percentage of respondents whose organization has an incident response plan, split by respondent country. *Asked to all respondents (1,800)*



Why are organizations not making progress with their information security preparedness, especially given the stringent GDPR regulations that came into effect as this report was released? There are cultural issues that require a fundamental change in the way that businesses communicate and organize themselves. Culture changes with leadership; so let's look at how leaders are shouldering the responsibility for security.

Responsibility for day-to-day security doesn't seem to fall on any one person's shoulders among our response base. 22 percent of organizations said that the CIO was ultimately responsible for security, compared to 20 percent for the CEO and 19 percent for the CISO. 15 percent thought that the buck stopped with the IT director.

It is a concern that one in five CEOs is ultimately managing a specialist task like day-to-day security. Are they being spread too thin, and are one in five of them truly able to oversee a security function in addition to other critical corporate tasks?

The narrow gap between these three roles shows that no one executive function is stepping up to the plate. It could be a sign of unclear separation between the CIO and CISO though. Often they are the same or collaborate closely.

A notable exception was Singapore, which seems to have elevated the CISO role. In that country, 33 percent of respondents gave that executive position primary responsibility for day-to-day security.

One thing is clear; while more people see the need for regular boardroom security discussions, their companies are failing to raise it sufficiently at C-suite level. 81 percent of respondents agreed that preventing a security attack should be a regular boardroom agenda item, up from last year's 73 percent. Only 61 percent said that it was, an increase from last year's 56 percent.

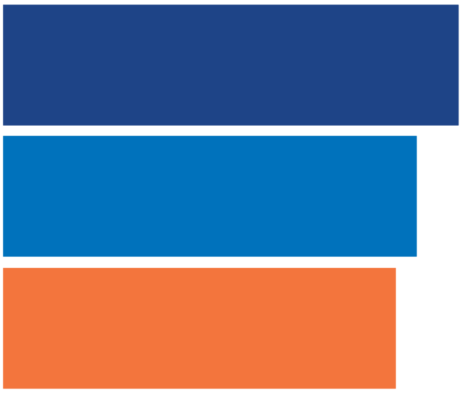
Data security is poor

With a lack of cohesion at the top, organizations are still struggling to secure their most important digital assets. Fewer than half (48 percent) said that they had fully secured all their critical data. With the GDPR now in effect, improvement isn't just an opportunity – it's mandatory. The US bucked the trend, with 61 percent of respondents saying that they had secured all their critical data.

One thing has improved. Companies are starting to take control of their data as cloud computing best practices mature.

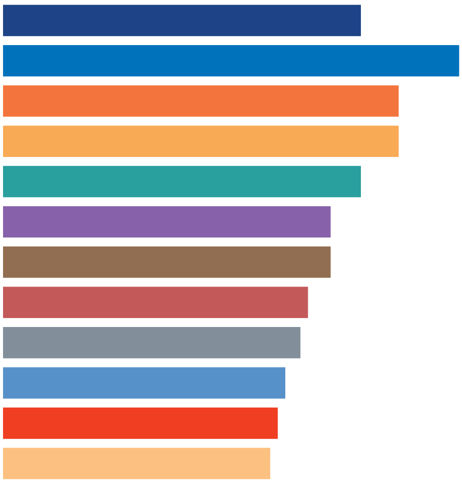
Respondents are also keeping data close to home. There is a strong tendency for an organization to store its data within its national borders. This trend could be driven by a combination of regulatory worries, data center ownership, and simple convenience.

Figure 7 Analysis showing the three most likely job roles to be ultimately responsible for managing respondents' organizations day-to-day security. *Asked to all respondents (1,800)*



22% CIO (Chief Information Officer)
20% CEO (Chief Executive Officer)
19% CISO (Chief Information Security Officer)

Figure 8 Analysis showing the percentage of respondents who would consider all of their organization's critical data, and all of their organization's data more generally, to be completely secure. *Asked to all respondents (1,800)*



48% Total
61% US
53% France
53% UK
48% Australia
44% Benelux
44% Norway
41% Germany and Austria
40% Switzerland
38% Sweden
37% Hong Kong
36% Singapore

Mistakes in business can happen when there are gaps in responsibility, which is why it is particularly worrying that a large percentage of respondents (43 percent) viewed security as the IT department's problem. The most prominent split here was between the 52 percent of C-suite executives that held this view, compared to the 39 percent of non-C-level employees who did. The division is just another indicator that senior management isn't taking security seriously enough as a cross-disciplinary challenge.

Insider threats are an organization's most significant weakness

The C-suite was far from the weakest spot, though. At the top of the list were third parties, such as contractors and temporary workers. 60 percent of respondents factored this group among the top three. Other research echoes these findings. For the first time, NTT Security's 2018 GTIR Report highlights Business and Professional Services as one of the top five sectors most targeted by attacks. These companies are a route into larger businesses.

We can combine third parties with the entire workforce, which came in second at 54 percent, as both often have privileged access to internal information and computing resources. Together, they comprise the insider threat category, which stands out as the most prescient security weakness in an organization today.

Insider threats are not necessarily malicious. People are a natural weakness because, as we have already seen, so few of them have a security policy to follow and those that do are often unaware of it. These insiders are often well meaning but make mistakes, opening attachments that install malware, following phishing links and downloading malicious apps.

The judicious use of protective technologies, including identity and access management and anti-malware technologies can help to keep people from inadvertently giving away access to critical data.

Figure 9 Analysis showing the percentage of respondents who agree that security is the IT department's problem and not the wider business. *Asked to all respondents (1,800)*

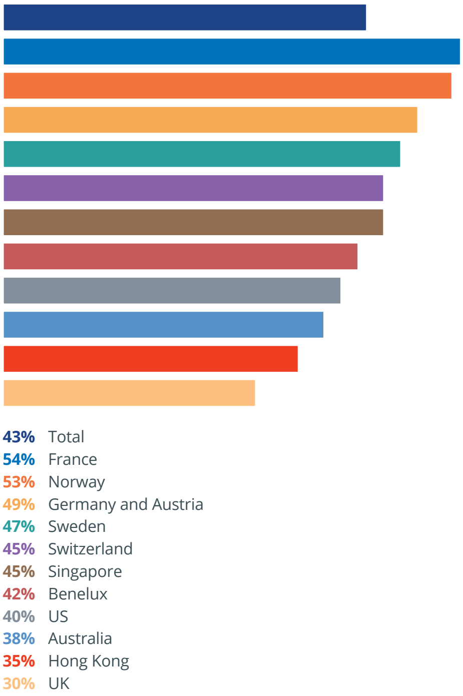
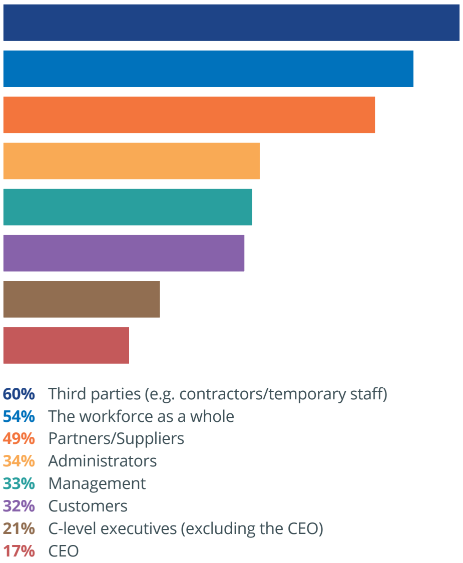


Figure 10 "In your organization, who do you think is the weakest security link?" *Asked to all respondents (1,800)*



Only one percent of respondents currently use a third-party managed security services provider. But more than one in three (37 percent) plan to. Of those, one in five (18 percent) cite a lack of skills as the main reason, with those in APAC more likely to lack the necessary skills (23 percent) compared to EMEA (18 percent) and the US (12 percent). Organizations still face challenges in recruiting the right people to manage security. Nevertheless, things are better than last year, when 28 percent of those moving to managed security services cited skills as an issue.

Companies aren't executing on cybersecurity insurance

38 percent of respondents have a dedicated cyber insurance policy, which is roughly in line with last year's 40 percent. One in five this year (21 percent) say that they are working towards getting one, which is down one percent on last year's 22 percent. These numbers suggest that the one in five organizations which annually vow that they are going to get a policy, is not following through. In terms of actually having a dedicated cybersecurity insurance policy in place, the US is noticeably more advanced than other regions, though, at 54 percent compared to APAC's 38 percent and EMEA's 34 percent.

What stands in their way? Cyber risk insurance is still a young field, and insurance companies continue to grapple with risk management and client evaluation issues. Getting these policies right isn't easy, and insurers are watching cyber attack-based data breaches rise. Just 40 percent of respondents confirm that their company insurance covers them for both data loss and an information security breach.

What could invalidate their company insurance? Failure to patch systems stood out as the highest concern, at 47 percent. The lack of an incident response plan (36 percent) and lack of employee care (29 percent) also scored highly. Nothing could highlight more clearly the urgency of formalizing and communicating information security policies and breach response plans.

Figure 11 Analysis showing the proportion of respondents who agree with the following statement: "We do not have adequate resources/skills in-house to cope with the number of security threats." *Asked to all respondents (1,800)*

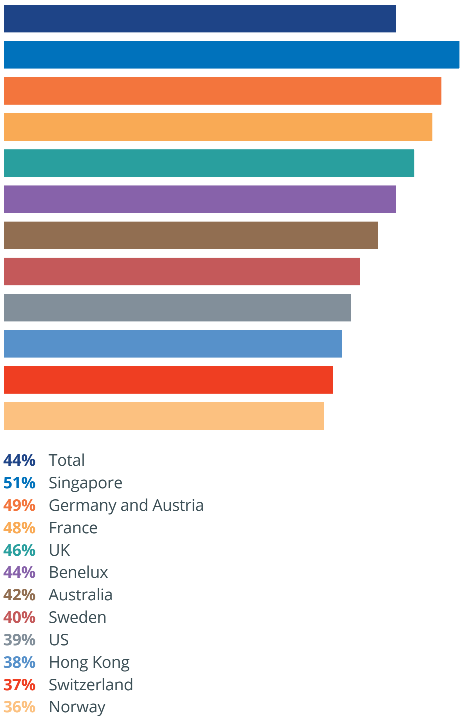
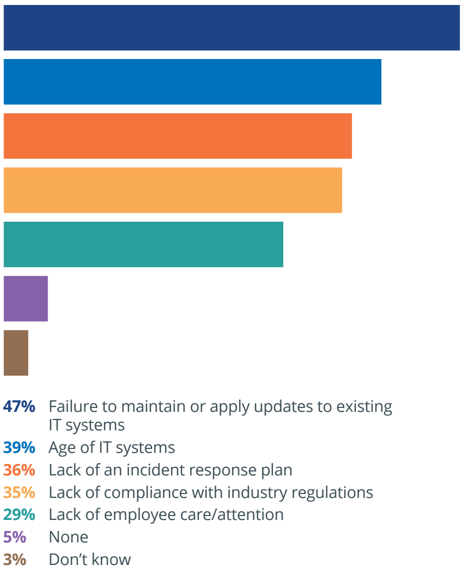


Figure 12 "For which of the following, if any, do you feel would or could invalidate your company insurance?" *Asked to respondents from organizations that are covered for data loss and information security breaches (1,301)*



Conclusion

Data breaches are becoming more severe, yet many organizations still assume they will never suffer one.

A lack of clear leadership at board level, combined with a tendency to hand-off responsibility for information security entirely to the IT department, creates the perfect conditions for an attacker to prove them wrong.

NTT Security was surprised at the number of respondents willing to wait for a ransom demand to arrive before tackling cybersecurity investment. These organizations will be among the most likely to fall victim to cyber attacks, and may find that ransoms aren't an option, or that criminals do not honor them.

In cybersecurity as in medicine, prevention is better than cure. NTT Security advises companies to follow both the spirit and the letter of regulatory guidelines, paying attention to how they evaluate risk and prepare for the time when hackers come calling.

1. *https://www.theglobeandmail.com/report-on-business/international-business/us-business/equifax-data-breach-could-become-the-most-costly-in-corporate-history/article38180834/*

2. *https://www.theverge.com/2017/7/12/15962520/verizon-nice-systems-data-breach-exposes-millions-customer-records*

3. *https://www.reuters.com/article/us-hudson-s-bay-databreach-shares/hudsons-bay-shares-drop-after-security-breach-at-saks-lordtaylor-stores-idUSKCN1H917N*

4. *https://www.nttsecurity.com/en-uk/landing-pages/2018-gtir*

NTT Security

Research demographics

Commissioned by NTT Security, the 2018 Risk:Value report research was conducted by Vanson Bourne in February and March 2018. 1,800 non-IT business decision makers were surveyed in the US, UK, Germany, Austria, Switzerland, France, Benelux, Sweden, Norway, Hong Kong, Singapore and Australia. Predominantly, organizations had more than 500 employees and were selected across a number of core industry sectors.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis, is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit **www.vansonbourne.com**

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **http://www.ntt.co.jp/index_e.html** to learn more about NTT Group.

www.nttsecurity.com